

NCP Secure Enterprise Client (Win32/64)

Service Release 9.30 Build 102

Date: January 2012

1. New Features and Enhancements

None

2. Changes Made and Problems Resolved

The following problems have been resolved:

Error when setting routes in split-tunneling

In some cases routes were incorrectly set when using split-tunneling.

Error when updating from 9.0 to 9.3

The corresponding update package has been modified.

3. Known Issues

Additional Ports in Hotspot Configuration

The functionality that uses the definition of additional ports within the hotspot configuration will fail under certain circumstances.

This error only occurs when the hotspot login must initially be established via a specific port – such as 8080.

In the case of conventional, public hotspots this error does not occur as here a default web browser request to port 80 or 443 on the server is redirected to the hotspot login page. In this case, the additionally configured ports can be used.

4. Getting Help for the NCP Secure Enterprise Client (Win32 / 64)

To ensure that you always have the latest information about NCP's products, always check the NCP website at:

<http://www.ncp-e.com/en/downloads.html>

For further information about the Enterprise Client, visit:

<http://www.ncp-e.com/en/products/central-managed-vpn-solution/remote-access-vpn-management.html>

For further assistance with the NCP Secure Enterprise Client (Win32/64), visit:

<http://www.ncp-e.com/en/about-us/contact.html>

Mail: <mailto:helpdesk@ncp-e.com?subject=A: NCP Secure Enterprise Client - Helpdesk message>

Release Notes



5. Features List

Central Management

As the **Single Point of Management**, NCP's Secure Enterprise Management (SEM) provides functionality and automation for the rollout, commissioning and efficient use of Secure Enterprise Clients. The Secure Enterprise Management (SEM) makes use of a VPN connection or the LAN (when on the company network), to automatically provide NCP Secure Enterprise Clients with:

- configuration updates,
- certificate updates, and
- updates to the Update Client.

Network Access Control / Endpoint Security

The policies for Endpoint Security (Endpoint Policy Enforcement)) are created centrally at the Secure Enterprise Management (SEM) and each NCP Secure Enterprise Client is only permitted access to the company network in accordance with the corresponding rules.

High Availability Services

The NCP Secure Enterprise Client supports the NCP HA Services. These services are client server based and can be used in two different operating modes: load balancing or failsafe mode. Regardless of the load on the server or whether a server has failed, the VPN connection to the corporate network is established and maintained reliably, in the background and without any delay for the user of the NCP Secure Enterprise Client.

Operating Systems

Microsoft Windows (32 & 64 bit): Windows 7, Windows Vista, Windows XP

Security Features

Support of the Internet Society's Security Architecture for IPsec and all the associated RFCs.

Virtual Private Networking

- RFC conformant IPsec (Layer 3 Tunneling)
 - IPsec Tunnel Mode
 - IPsec proposals are negotiated via the IPsec gateway (IKE Phase 1, IPsec Phase 2)
 - Communication only in the tunnel
 - Message Transfer Unit (MTU) size fragmentation and reassembly
 - Network Address Translation-Traversal (NAT-T)
 - Dead Peer Detection (DPD)

Authentication

- Internet Key Exchange (IKE):
 - Aggressive Mode and Main Mode, Quick Mode
 - IKEv2 incl. MOBIKE
 - Perfect Forward Secrecy (PFS)
 - IKE Config. Mode for dynamic allocation of private IP (virtual) address from address pool

- Pre-shared secrets or RSA Signatures (and associated Public Key Infrastructure)
- User authentication:
 - User Authentication via GINA/Credential Management
 - Windows Logon over VPN connection
 - XAUTH for extended user authentication
 - One-time passwords and challenge response systems
 - Authentication details from certificate (prerequisite PKI)
- Support for certificates in a PKI:
 - Soft certificates, Smart cards, and USB tokens: Multi Certificate Configurations
- Seamless rekeying
- PAP, CHAP, MS CHAP v.2
- Pre-Authentication (Authentication before VPN establishment)
- IEEE 802.1x:
 - Extensible Authentication Protocol – Message Digest 5 (EAP-MD5): Extended authentication relative to switches and access points (layer 2)
 - Extensible Authentication Protocol – Transport Layer Security (EAP-TLS): Extended authentication relative to switches and access points on the basis of certificates (layer 2)
- Secure hotspot logon using HTTP or EAP
- RSA SecurID ready

Encryption and Encryption Algorithms

Symmetrical: AES 128,192,256 bits; Blowfish 128,448 bits; Triple-DES 112,168 bits
Asymmetrical: RSA to 2048 bits, dynamic processes for key exchange

Hash / Message Authentication Algorithms

- SHA1, SHA-256, SHA-384, SHA-512, MD5
- Diffie Hellman groups 1, 2, 5, 14, 15-18 used for asymmetric key exchange and PFS

Public Key Infrastructure (PKI) - Strong Authentication

- X.509 v.3 Standard
- Entrust ready
- Support for certificates in a PKI
 - Smart cards and USB tokens
 - PKCS#11 interface for encryption tokens (smart cards and USB)
 - Smart card operating systems
 - TCOS 1.2, 2.0 and 3.0
 - Smart card reader systems
 - PC/SC, CT-API
 - Soft certificates
 - PKCS#12 interface for private keys in soft certificates
- PIN policy: administrative specification of PIN entry to any level of complexity
- Certificate Status Protocol (CSP) for the use of user certificates in the Windows certificate store
- Revocation:
 - End-entity Public-key Certificate Revocation List (EPRL formerly CRL)
 - Certification Authority Revocation List, (CARL formerly ARL)
 - Online Certificate Status Protocol (OCSP)
 - Certificate Management Protocol (CMP)ⁱ

Personal Firewall

- Stateful Packet Inspection
- IP-NAT (Network Address Translation)
- Friendly Net Detection (Firewall rules adapted automatically if connected network recognized based on its IP subnet address, the DHCP server's MAC address or an NCP FND serverⁱ)
- Supports secure hotspot logon feature
- Start application before or after VPN establishment
- Differentiated filter rules relative to:
 - Protocols, ports or IP addresses
 - LAN adapter protection,
 - Central administration (optional)ⁱⁱ
 - Protect VMware Guest systems
 - IPv4 and IPv6 support

Endpoint Security

- Endpoint Policy Enforcement ⁱⁱ

Networking Features

Secure Network Interface

- LAN Emulation
 - NCP Virtual Ethernet adapter with NDIS interface
 - Wireless Local Area Network (WLAN) support
 - Wireless Wide Area Network (WWAN) support

Network Protocol

- IP

Communications Media

- LAN
- Wi-Fi
- GPRS / 3G (UMTS, HSDPA), GSM (incl. HSCSD)
 - Windows 7 – Mobile Broadband support
 - Messaging Center (send & receive SMSs)
- xDSL (PPPoE)
- xDSL (PPP over CAPI, AVM)
- PSTN
- ISDN
- Automatic Media Detection (AMD)
- External Dialer
- Seamless Roaming (LAN / Wi-Fi / GPRS / 3G)

Dialers

- NCP Secure Dialer
- Microsoft RAS Dialer (for ISP dial-up using dial-up script)

Line Management

- Dead Peer Detection with configurable time interval
- Short Hold Mode
- Inactivity Timeout (send, receive or bi-directional)
- Channel Bundling (dynamic in ISDN) with freely configurable threshold value
- Wi-Fi Roaming (handover)
- Budget Manager
 - Separate management of Wi-Fi, GPRS/3G, xDSL, PPTP, ISDN and modem connections
 - Duration or volume based budgets
 - Management of GPRS/3G roaming costs
 - Separate management of multiple Wi-Fi access points

IP Address Allocation

- Dynamic Host Control Protocol (DHCP)
- Domain Name Service (DNS) : gateway selection using public IP address allocated by querying DNS server

VPN Path Finder

- NCP Path Finder Technology
 - Fallback to HTTPS (port 443) from IPsec if neither port 500 nor UDP encapsulation are available ⁱⁱⁱ

Data Compression

- IPsec Compression: lzs, deflate

Link Firewall

- Stateful Packet Inspection

Additional Features

- VoIP prioritization
- UDP encapsulation
- IPsec roaming ⁱⁱⁱ
- Wi-Fi roaming ⁱⁱⁱ
- WISPr support (T-Mobile hotspots)

Point-to-Point Protocols

- PPP over Ethernet
- PPP over GSM,
- PPP over ISDN,
- PPP over PSTN.
 - LCP, IPCP, MLP, CCP, PAP, CHAP, ECP

Standards Conformance

Internet Society RFCs and Drafts

Security Architecture for the Internet Protocol and assoc. RFCs (RFC2401 - 2409),

- Internet Key Exchange Protocol (includes IKMP/Oakley) (RFC 2406),
- Negotiation of NAT-Traversal in the IKE (RFC 3947),

- UDP encapsulation of IPsec Packets (RFC 3948),
- IKE Extended Authentication (XAUTH), IKE configure (IKECFG) and Dead Peer Detection (DPD)
- Additional Extended Key Usages:
 - id-kp-ipsecIKE (1.3.6.1.5.5.7.3.17) in accordance with RFC 4945
 - anyExtendedKeyUsage (2.5.29.37.0) in accordance with RFC 4945
 - IKEIntermediate (1.3.6.1.5.5.8.2.2) in accordance with draft-ietf-IPsec-pki-req-03

FIPS Inside

The Secure Client incorporates cryptographic algorithms conformant to the FIPS standard. The embedded cryptographic module incorporating these algorithms has been validated as conformant to FIPS 140-2 (certificate #1051).

FIPS conformance will always be maintained when any of the following algorithms are used for establishment and encryption of the IPsec connection:

- Diffie Hellman Group: Group 2 or higher (DH starting from a length of 1024 Bit)
- Hash Algorithms: SHA1, SHA 256, SHA 384, or SHA 512 Bit
- Encryption Algorithms: AES with 128, 192 or 256 Bit or Triple DES

Client Monitor

Intuitive Graphical User Interface

- Language support (English, German, French)
 - Monitor & Setup: en, de, fr
 - Online Help and License en, de
- Icon indicates connection status
- Client Info Center – overview of :
 - General information - version#, MAC address etc
 - Connection – current status
 - Services/Applications – process(es) – status
 - Certificate Configuration – PKI certificates in use etc.
- Configuration, connection statistics, Log-book (color coded, easy copy&paste function)
- Integrated support of Mobile Connect Cards (PCMCIA, embedded)
- Password protected configuration and profile management
- Trace tool for error diagnosis
- Monitor can be tailored to include company name or support information
- Custom Branding Option
- Internet Availability Tests

Notes

- i If you wish to download NCP's FND server as an add-on, please click here:
<http://www.ncp-e.com/en/downloads/software.html>
- ii Prerequisite: NCP Secure Enterprise Management
- iii Prerequisite: NCP Secure Enterprise Server V 8.0 and later

More information on the NCP Secure Enterprise Client (Win32/64) is available on the Internet at:
<http://www.ncp-e.com/en/products/central-managed-vpn-solution.html>

Release Notes

